

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI
SOUTHERN DIVISION**

IN THE MATTER OF THE SEARCH OF:

**A SILVER IN COLOR, NOKIA BRAND
MODEL C110 (N156DL) CELL PHONE
BEARING IMEI 350817214594890,
CURRENTLY LOCATED AT 321 EAST
CHESTNUT EXPRESSWAY,
SPRINGFIELD, MISSOURI 65802**

Case No. 24-SW-2144WJE

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Lee Walker, a Task Force Officer (TFO) with the Federal Bureau of Investigations (FBI),
being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been employed as a police officer with the City of Springfield, Missouri, since 2004. I am currently a TFO with the FBI, as well as a member of the Southwest Missouri Cyber Crimes Task Force (SMCCTF) in Joplin, Missouri. As a TFO, I have been assigned to investigate technology crimes involved sex offenses, including violations against children and sex offender compliance investigations. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have attended training provided by the Missouri Internet Crimes Against Children (ICAC) Task Force. I have written, executed, and assisted in over 100 search warrants on the state

and federal level. As a TFO with the FBI, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I am a “federal law enforcement officer” within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.

3. The statements in this affidavit are based on my personal observations, training and experience, investigation of this matter, and information obtained from other agents and witnesses. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, this Affiant has not included each and every fact known to me concerning this investigation. This affiant has set forth the facts necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2250(a), that is, a violation of the Sex Offender Registry and Notification Act (SORNA), are currently located within a silver in color, Nokia brand model brand C110 (N156DL) cellular phone bearing IMEI 350817214594890.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a silver in color, Nokia brand model brand C110 (N156DL) cellular phone bearing IMEI 350817214594890, hereinafter “the Device.” The Device is currently stored at the Springfield, Missouri, Police Department Cyber Crime Office, located at 321 East Chestnut Expressway, Springfield, Missouri 65802 in the Western District of Missouri.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B for a violation of 18 U.S.C. § 2250(a), that is, a violation of the Sex Offender Registration and Notification Act.

PROBABLE CAUSE

6. On May 1, 2024, the Affiant met with United States Probation and Parole Office (USPO) Supervisor and Search Coordinator Daniel Schepers. USPO Supervisor Schepers requested assistance with an individual being supervised by their office, Jeremy Green (hereinafter "Green"). Green was convicted in 2013, in San Diego, California, under the Uniform Code of Military Justice (UCMJ) of two counts of Rape of Child Under 12, three counts of Aggravated Sexual Contact of a Child, and two counts of Sodomy. The victims in Green's offenses of convictions were 12-year-old minors. As a result of the convictions, Green is under the supervision of the USPO, and he is subject to sex offender registration requirements under SORNA and under Missouri state law. Green's convictions make him a Tier III offender under SORNA.

7. On March 25, 2024, Green's supervising Probation Officer, USPO Officer Roxana Stone, requested a search of Green pursuant to conditions of his supervised release, which was approved by Chief USPO Brian Graham. The request was based on two failed polygraph examinations. Green failed a polygraph test conducted on January 18, 2024, and second exam on February 21, 2024, regarding questions about accessing the Internet on an unmonitored device.

8. On April 15, 2024, Green was contacted at his workplace, Diversified Plastics, located at 120 West Mount Vernon Street in Nixa, Missouri, a location within the Western District of Missouri. During this search, USPO Supervisor Schepers located the Device, a Nokia brand model C110 cellular device, on the driver's seat of Green's vehicle. The Device was unreported and not approved by the USPO. Green provided a PIN code of 2911 to unlock the Device. USPO Supervisor Schepers conducted a non-forensic, cursory hand search of the Device. The phone number for the device was identified as (417) 306-4338. The phone contained a large volume of social media accounts and adult pornography, including the following:

- a. Google email accounts: vagitarian851@gmail.com (username Darren Cross); crosssaaron00@gmail.com (username Aaron Cross);
- b. Zangi: account under username “Darren Cross”;
- c. YouTube: account under username “Darren Cross”;
- d. Google Meet and Google Chat: both accounts under username “Darren Cross”;
- e. Facebook: account under username “Darren Cross”;
- f. Signal: account under username “Vagitarian851”;
- g. SnapChat: account under username “Darren_Cross2024”;
- h. Telegram: account under username “Darren”; and
- i. Tiktok

9. USPO Supervisor Schepers seized the Device, and ceased his cursory examination. On May 1, 2024, USPO Supervisor Schepers transferred custody of the Device to the Affiant, who secured the Device at the FBI Springfield RA Office. On May 2, 2024, the Affiant transferred the Device to the SPD Cyber Crime Office, where it is currently inventoried and secured.

10. This Affiant reviewed Green’s most recent registration, which covered the period of April 2024. Green was registered with Douglas County, Missouri, Sheriff’s Office, as that is where his residence is located, and that is a location within the Western District of Missouri. Green signed the acknowledgement that he had read and understood the Missouri sex offender registry requirements. Specifically, he acknowledged that he understood and agreed “I will abide by all registration requirements set forth in the Statutes, 598.400-589.426 RSMo, and the Federal Adam Walsh Act. Failure to comply with offender registration requirements is a criminal offense. (589.425 RSMo).” Green did not list the phone number for the Device, nor did he report any of the social media accounts located on the Device.

11. Green is required under SORNA to correctly maintain and update his sex offender registration in the jurisdiction in which he resides, works, or is a student in. Under Missouri laws, Section 589.141.2(4), Revised Missouri Statutes, requires a sex offender to list “Email addresses, instant messaging addresses, and any other designations used in internet communications, postings, or telephone communications.”

12. This Affiant believes that a forensic examination of the Device will contain evidence that Green has violated provisions of SORNA.

TECHNICAL TERMS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Computer: The term “computer” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

b. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending,

receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

c. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

d. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some

GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

f. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

g. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function

as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

h. **Pager:** A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

i. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

j. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, computer, digital camera, portable media player, GPS, and PDA. In my training and experience, examining data stored on devices of this

type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.


18. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION


20. I submit that this affidavit supports probable cause for a search warrant authorizing

the examination of the Devices described in Attachment A to seek the items described in Attachment B.



Lee Walker
Task Force Officer
Federal Bureau of Investigation

Sworn to and subscribed to before me in my presence via telephone, or by other reliable electronic means, on this 1st day of July 2024.



THE HONORABLE WILLIE J. EPPS, JR.
Chief United States Magistrate Judge
Western District of Missouri